

IEEE - Cedar Rapids Section
FALLCON 2004



Securing Wireless Networks by Wireless Honeynets

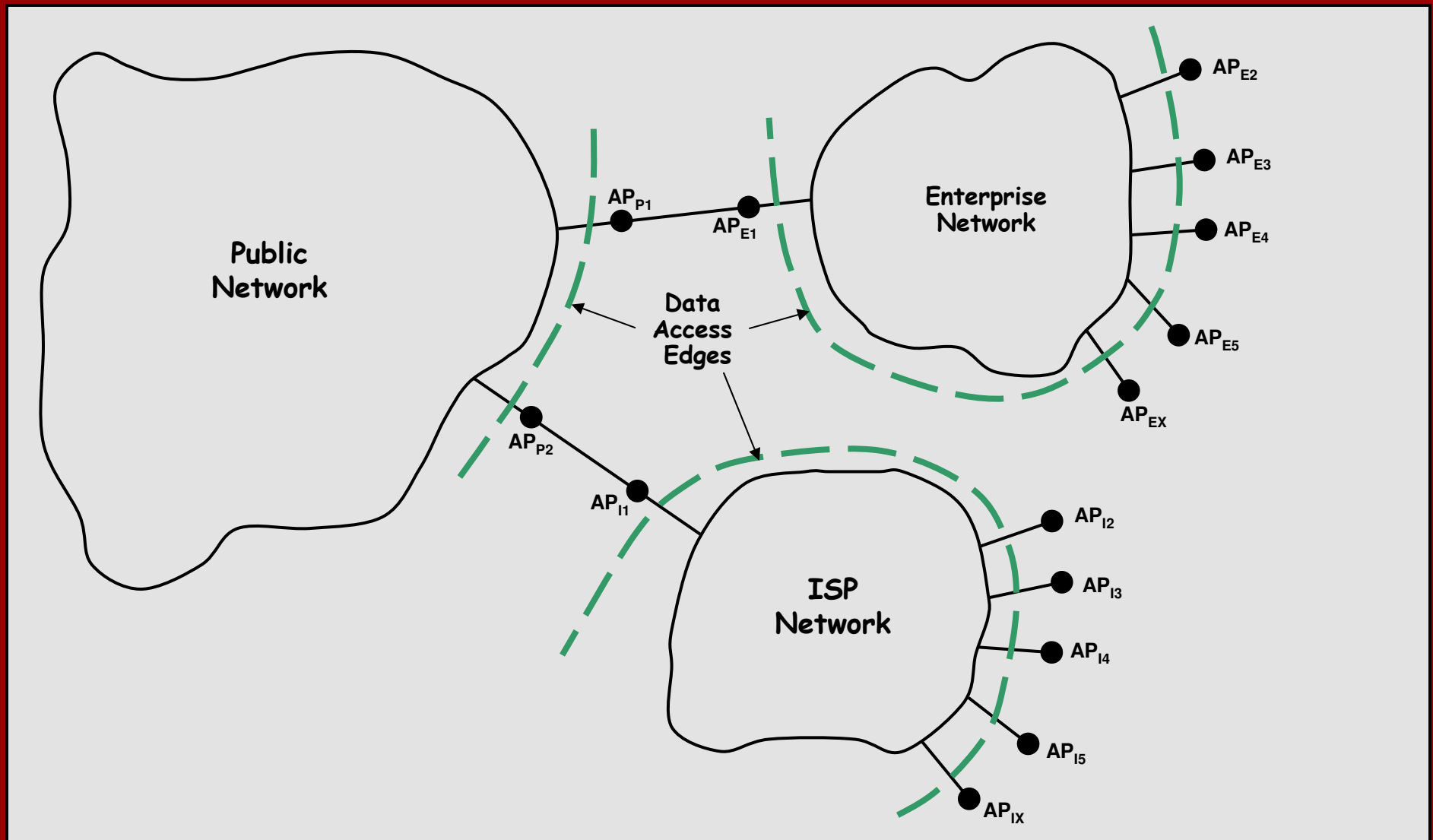
Steve F. Russell
Associate Professor
Iowa State University
sfr@iastate.edu
October 27, 2004

October 25-26, 2004
Kirkwood Training & Outreach
Center
3375 Armar Drive
Marion, Iowa

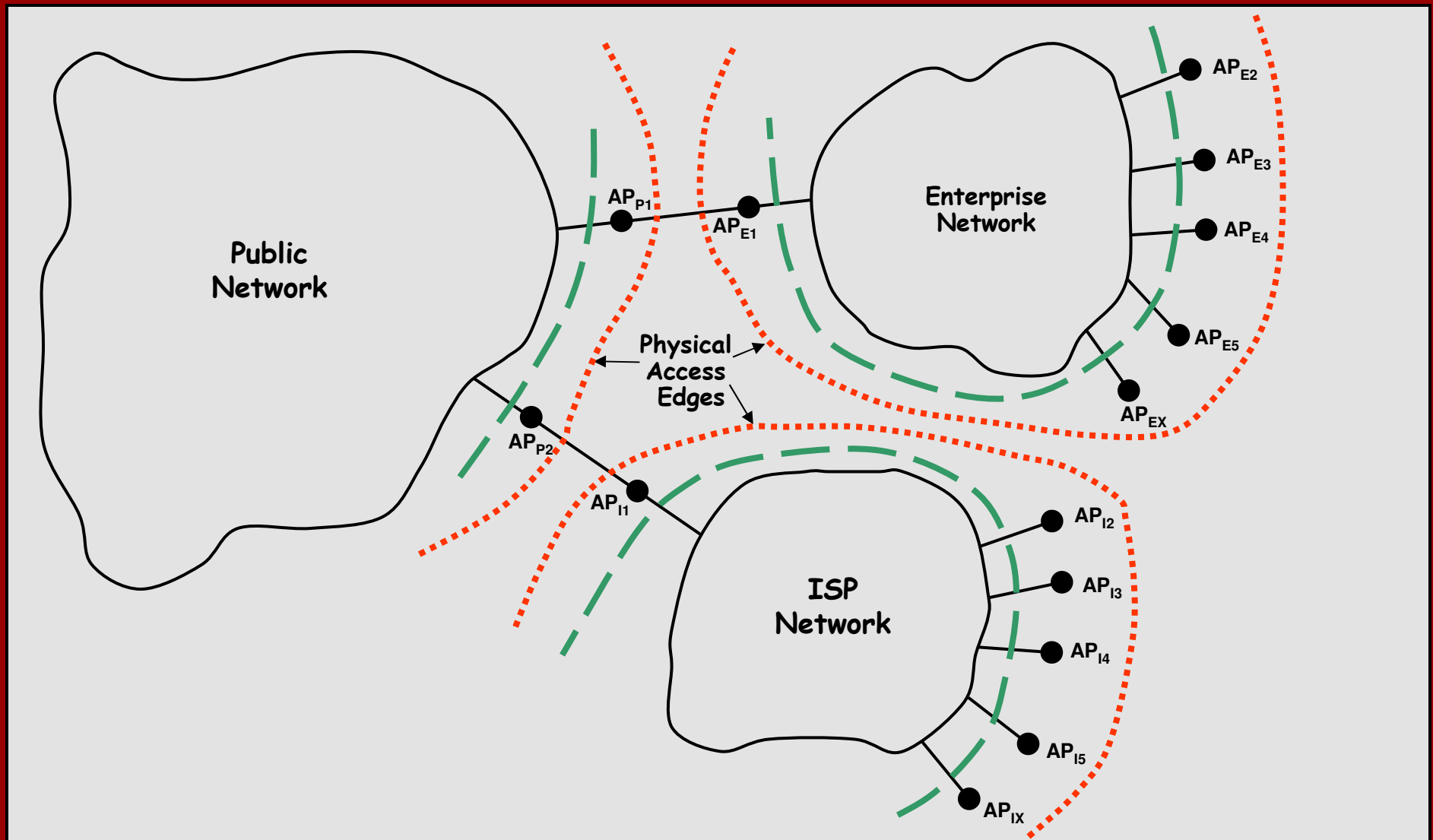
Abstract

This paper describes a new concept of protecting a geographic area, or physical facility, and its associated wireless network, from aggressive wireless intrusion attacks when the attacker is outside the enterprise network or is just penetrating the network edge. In contrast to the traditional honeypot, this new concept, called a wireless honeynet, spoofs airlink mobility and wireless traffic in addition to spoofing wired network traffic and server access. We want to detect the intrusion, monitor and characterize the progress of the intrusion and, at some point, stop the intrusion. When fully implemented, the wireless honeynet will incorporate imposter mobiles, position-location, geographic information systems, and zone jammers.

Traditional Wired-Network Data-Access Edges

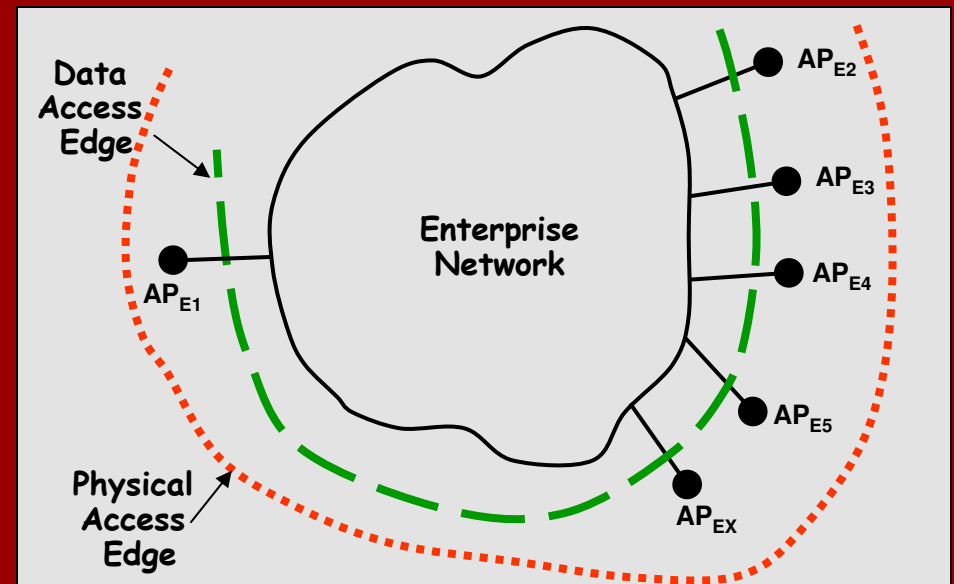


Traditional Wired-Network Physical-Access Edges



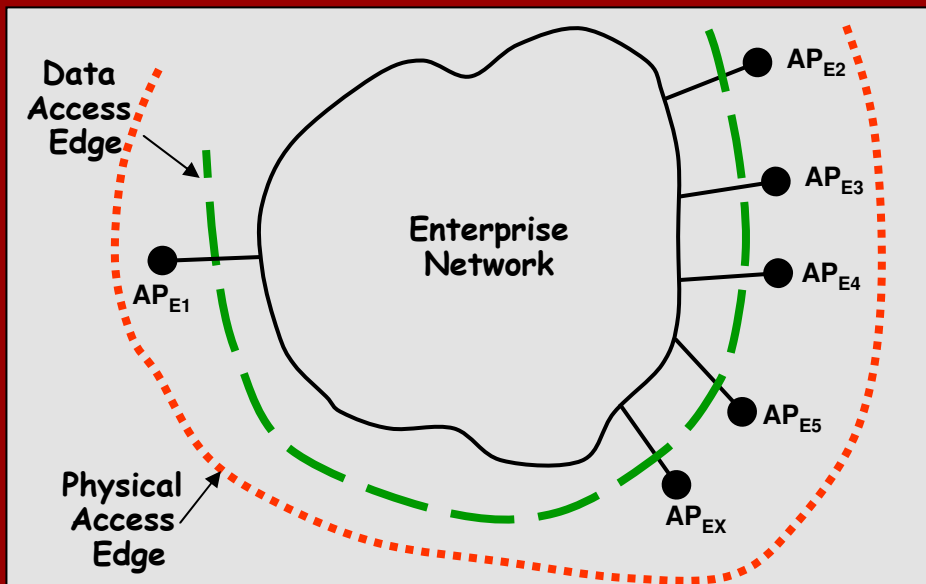
Good Internal Security Measures

- AP_{E1} Access Management
 - **Firewall/NAT**
- Internal Network Security Management
 - “need to know” firewalls and NAT partitioning
- AP_{EX} Access Management
 - **Limited physical access**
 - **User authentication**



Traditional Access Security/Privacy Measures

- Physical Access Management
- Switches – not hubs
- IP Management
- MAC Authorization
- User Authorization
- Virtual Private Network



WLAN Connection Choices

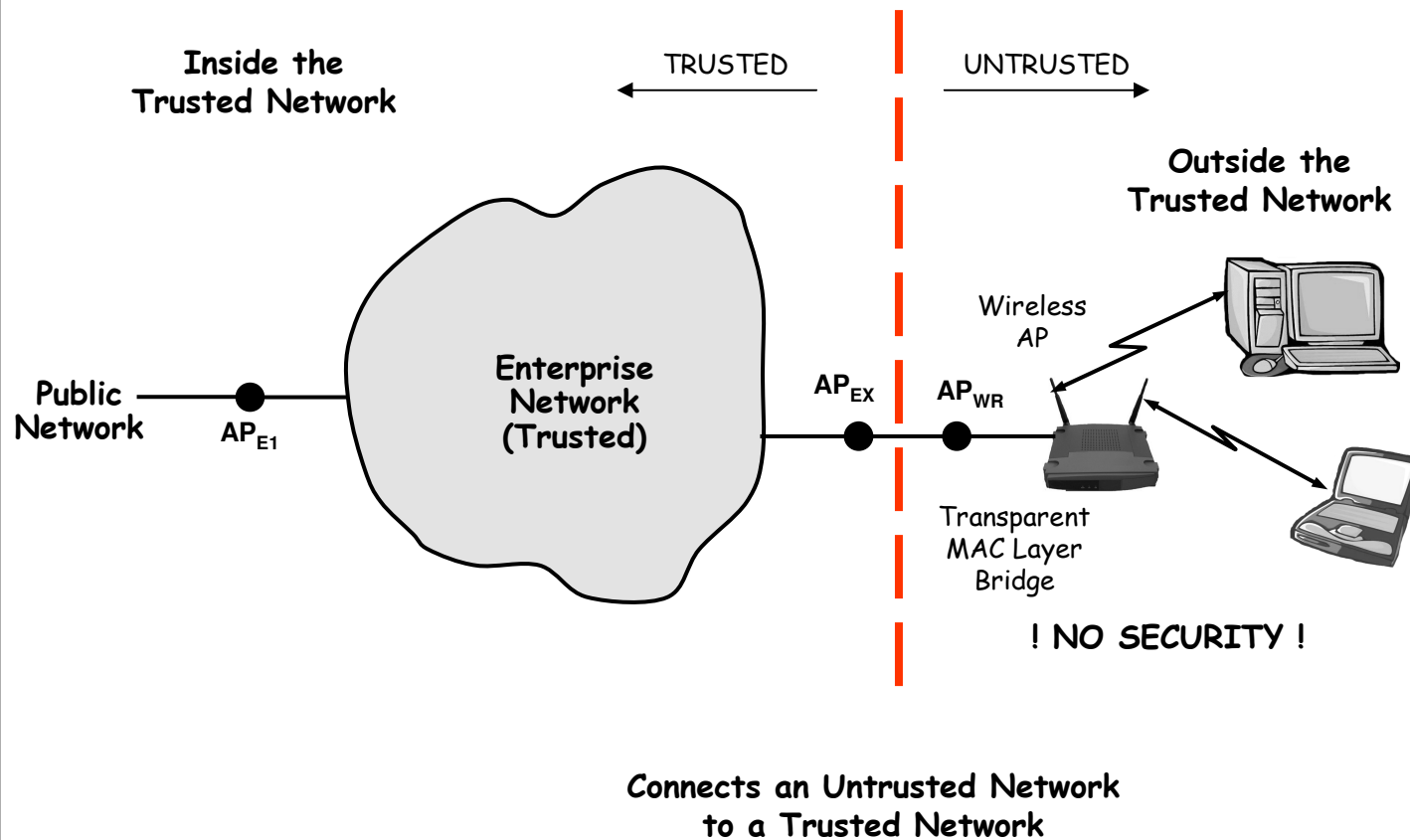
- Rogue Access Point
- Mobile/Portable Ad Hoc WLANs
- Bridges
 - **Point to point**
 - **Point to multipoint**
- Repeaters
- Infrastructure Connected WLANs – Inside the trusted network
- Infrastructure Connected WLANs – Outside the trusted network

The Ubiquitous Wireless Access Point

- Install “out of the box”
 - Rogue access point
 - Transparent MAC-Layer Bridge
 - No security
 - Not a good choice!

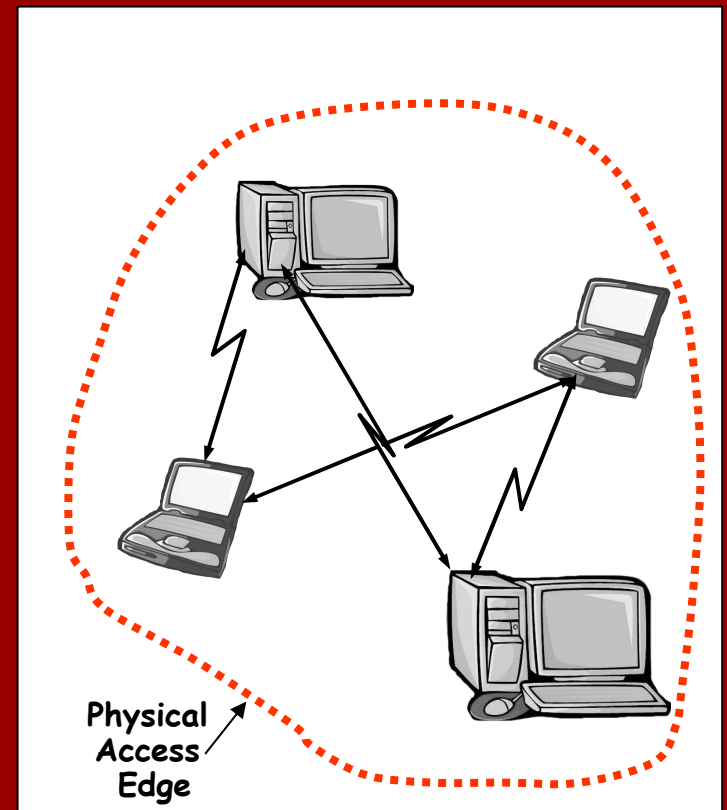


Rogue Access Point

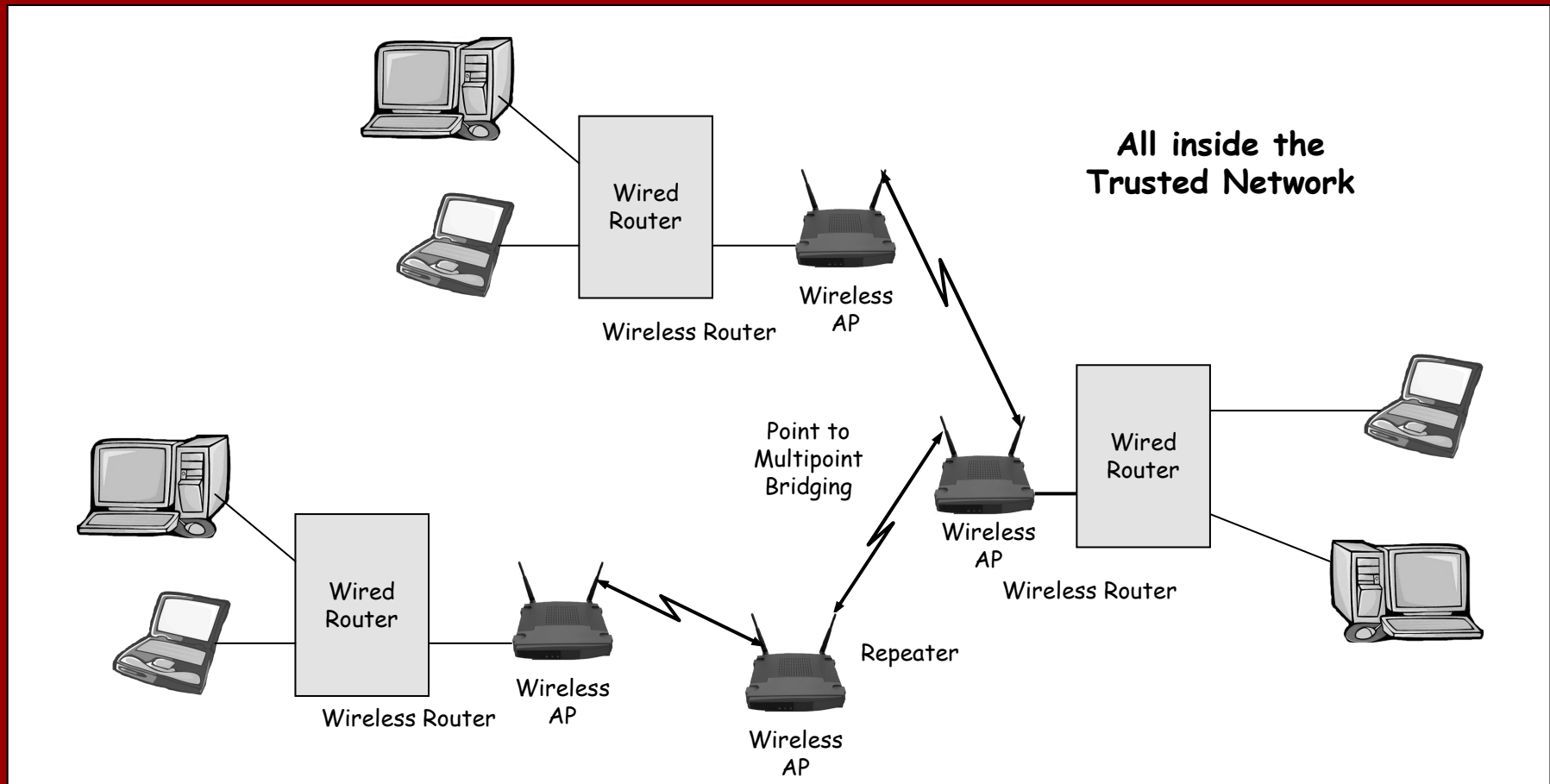


Mobile/Portable Ad Hoc WLANs

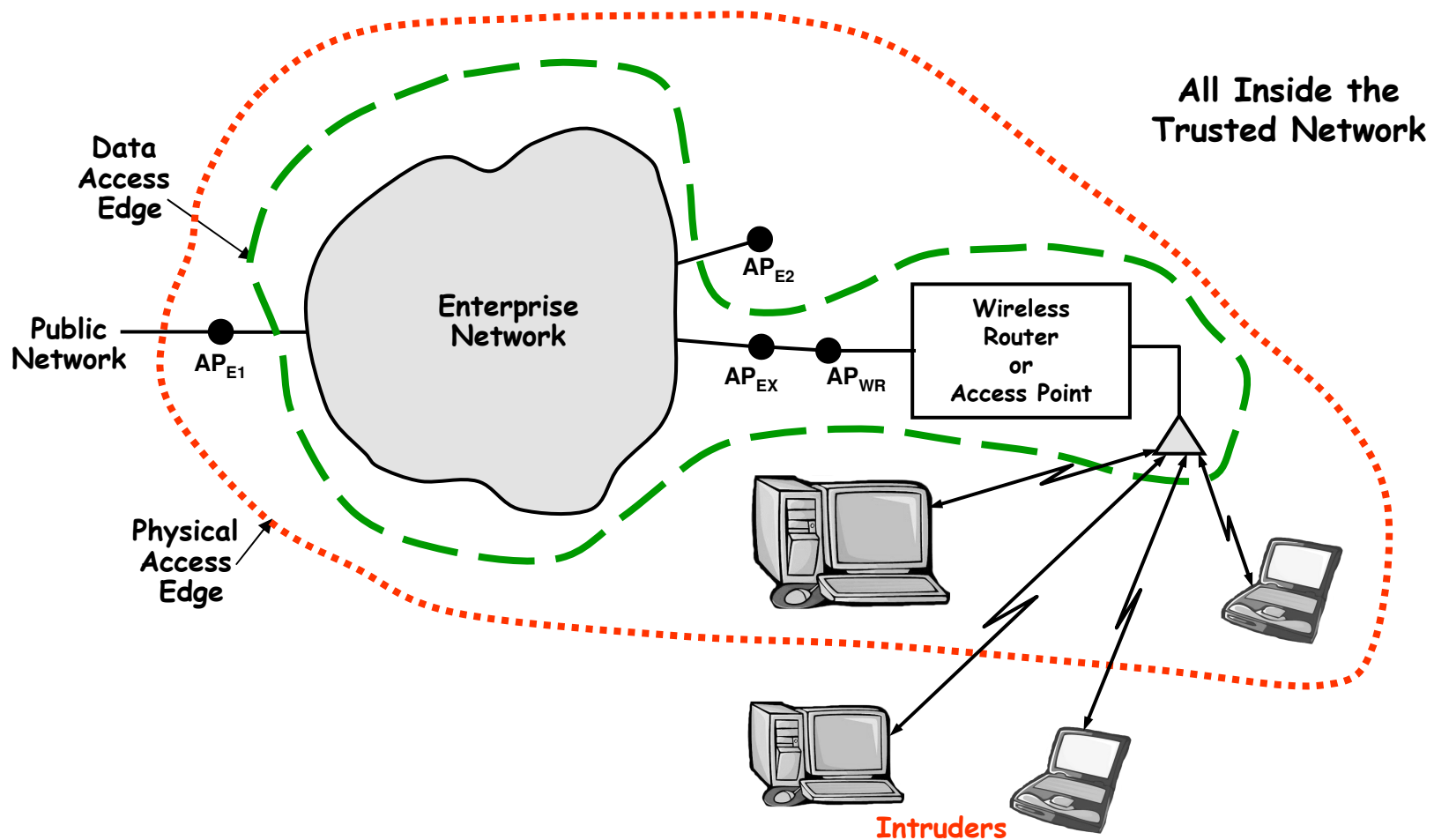
- NIC to NIC wireless link
- NIC-level security
- User maintained security
- “Hot” research area
 - **Mobile Ad Hoc Networks (MANETs)**



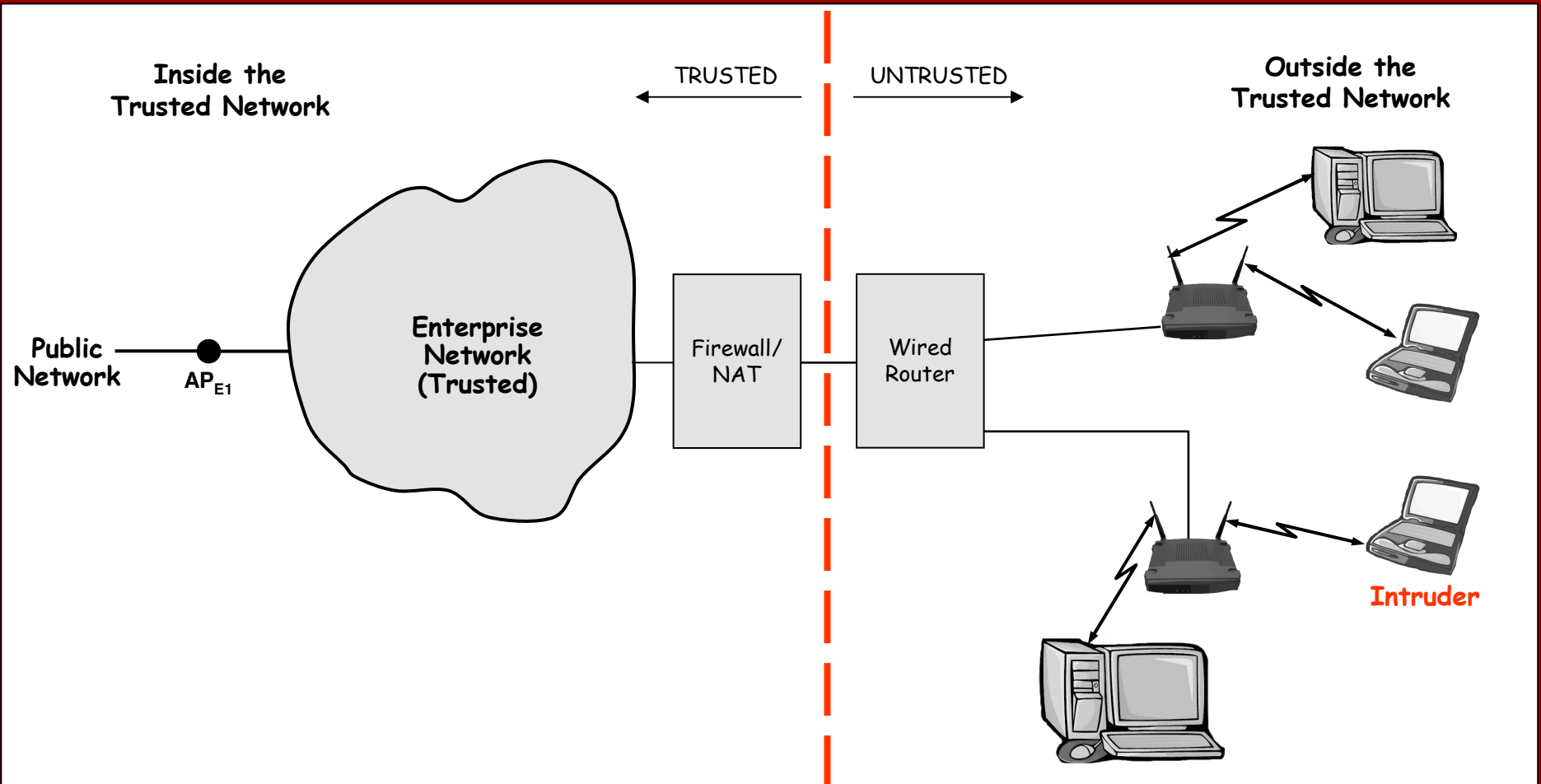
Wireless Bridges and Repeaters



Infrastructure Connected WLANs Inside the trusted network



Infrastructure Connected WLANs Outside the trusted network



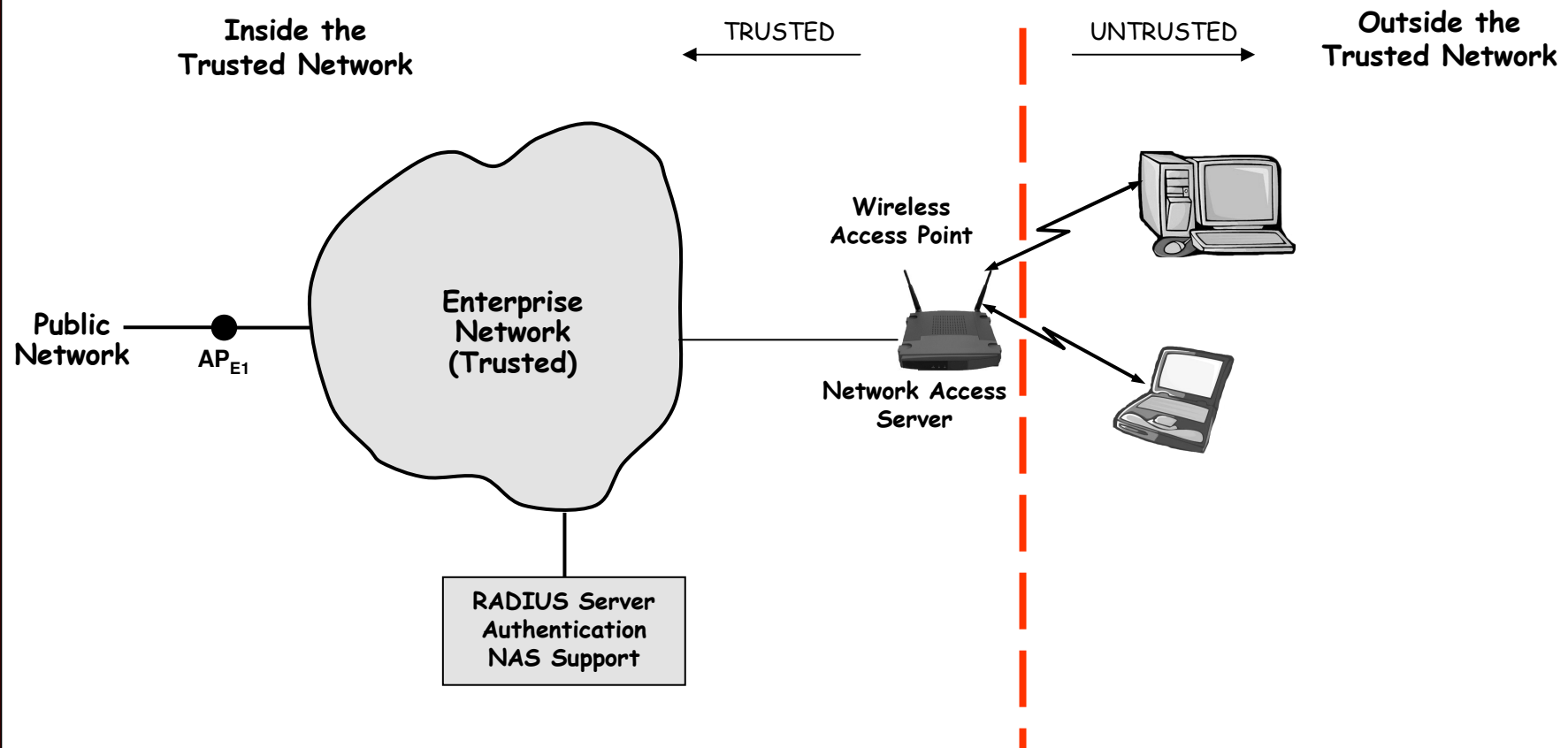
WLAN Security Issues – Airlink Security (Wireless Access Point Security)

- **Airlink intrusion Security**
 - Wired equivalent privacy
 - WiFi Protected Access
 - RADIUS: Authentication, authorization, and access control
 - Two-way (Mutual) Authentication
- **Airlink eavesdropping Security**
 - Wired equivalent privacy
 - WiFi Protected Access
- **Airlink denial of access (DOA) Security**
 - Anti-interference, anti-jam
- **Rogue Access point**
 - Rogue AP detection

WLAN Security Issues – System Security

- **User authorization**
 - Username-Password
- **User identification**
 - IP
 - MAC
 - Electronic Fingerprint
- **User Privacy**
 - Virtual Private Network (VPN)

Wi-Fi Protected Access (WPA) with RADIUS Server

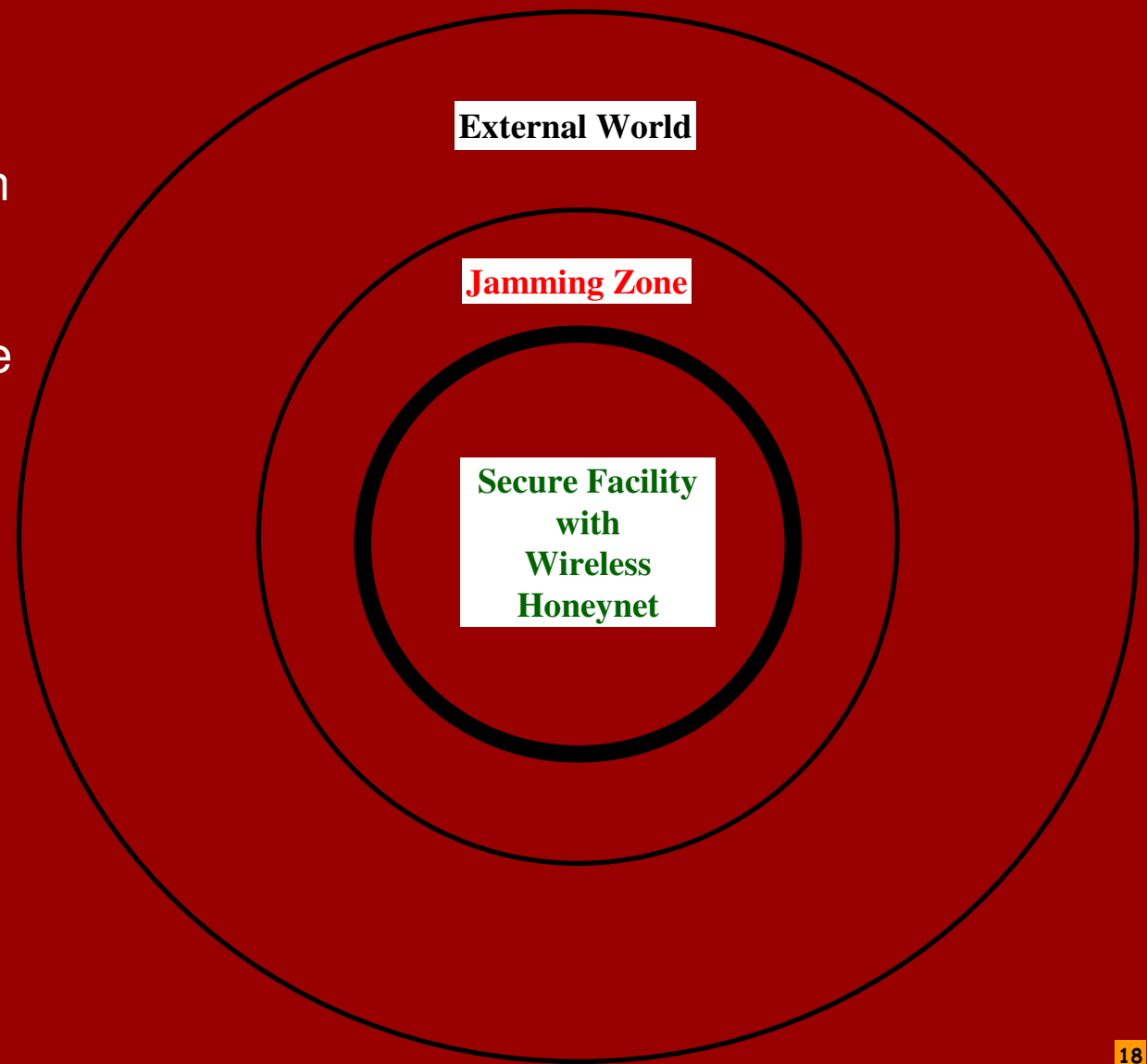


Future Wireless Security Technologies

- **Electronic Fingerprinting of wireless NICs and access points**
 - DILON project at Iowa State
- **Wireless Honeynets**
 - Honeynet project at Iowa State
- **Wireless coverage area management with high-gain antennas**

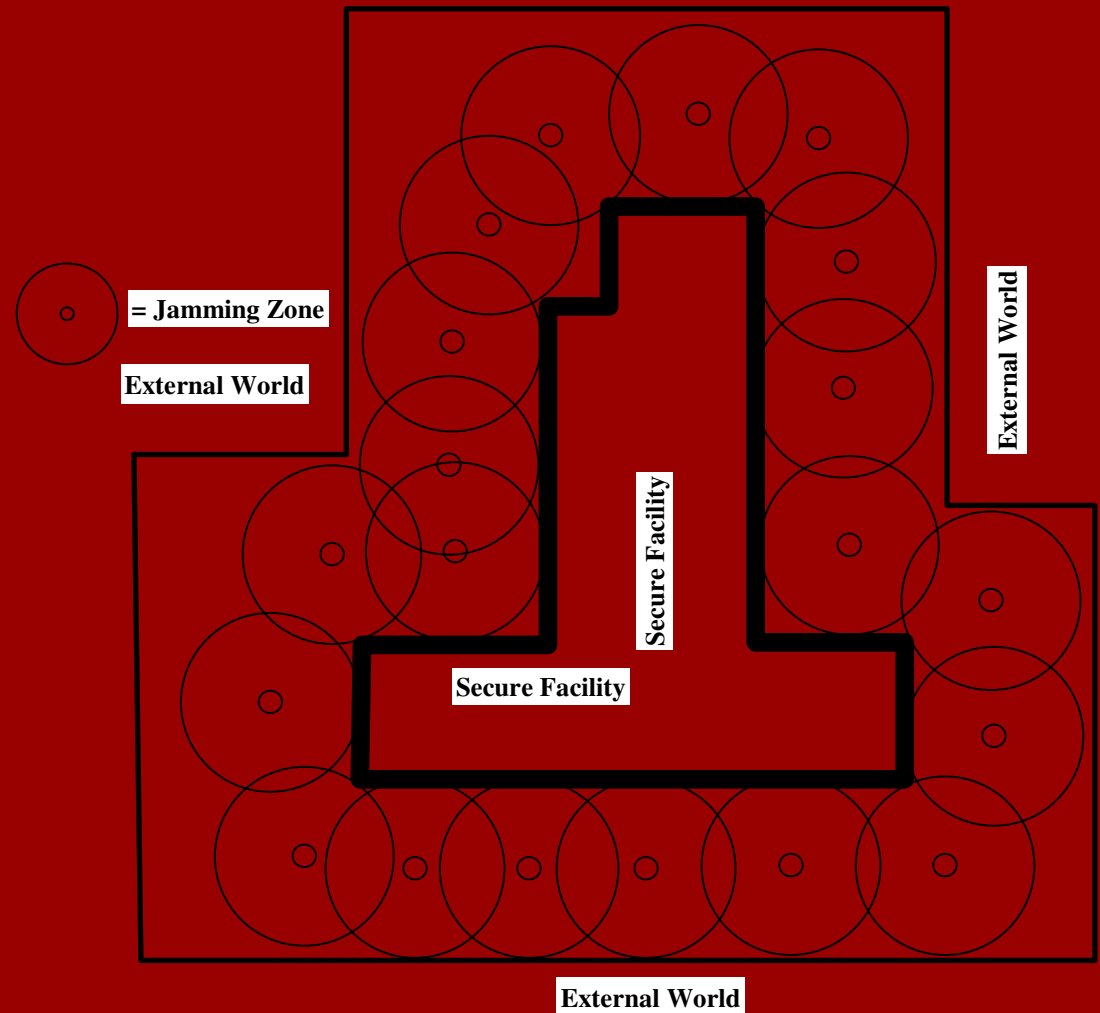
Wireless Honeynet Concept

- Imposter network with mobile access points, honeypots and intrusion analysis
- Position Location of intruder NICs and rogue access points
- Jamming of wireless intruders
- Spoofing of network traffic and behavior
- Area-of-coverage management



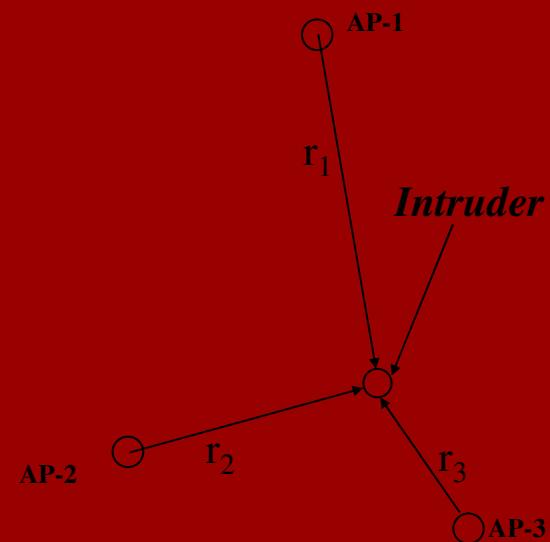
Wireless Honeynet – Jamming Zone

- Low-Power “parking-lot” jammers
- Directional antennas

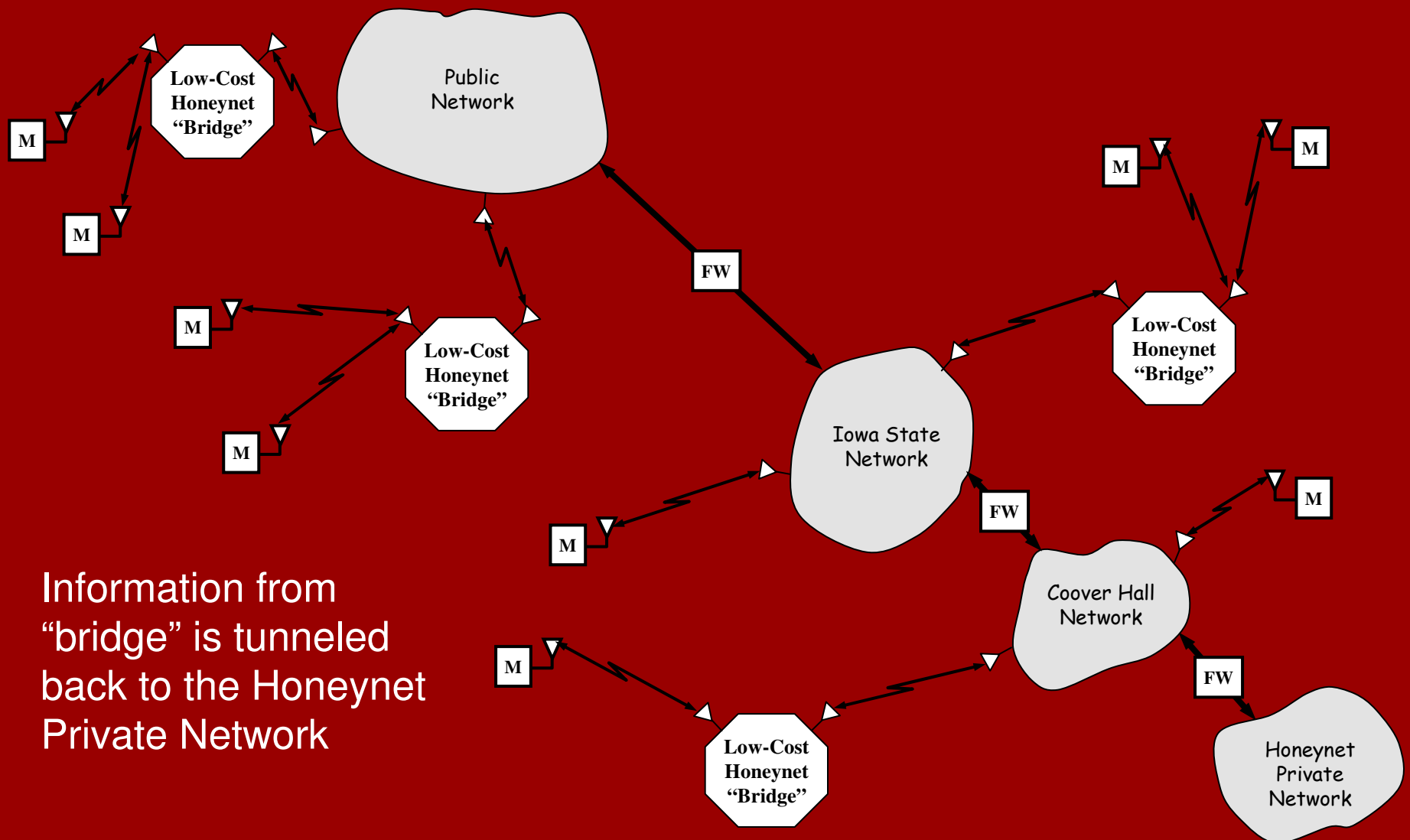


Honeynet Position-Location

- Position-Location by signal strength triangulation

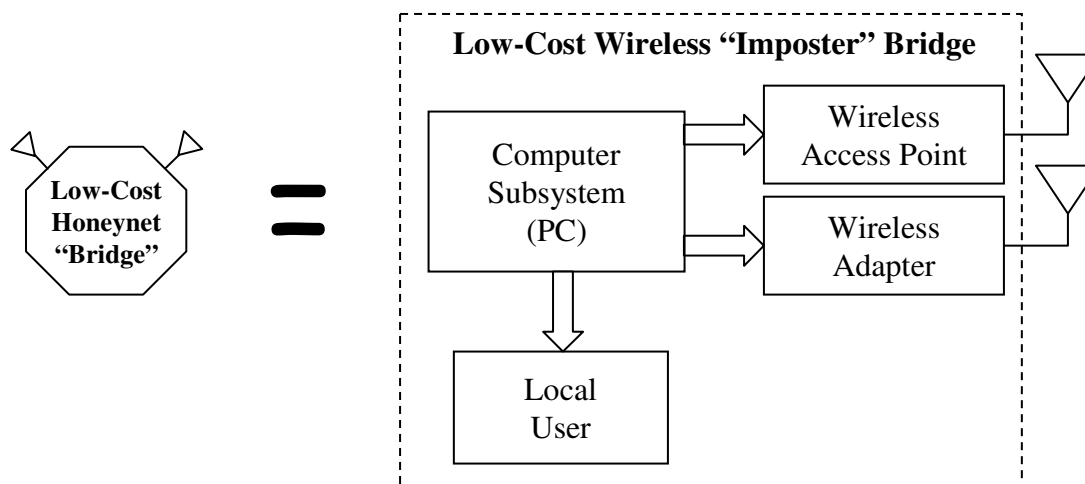


Iowa State Honeynet Testbed Concept

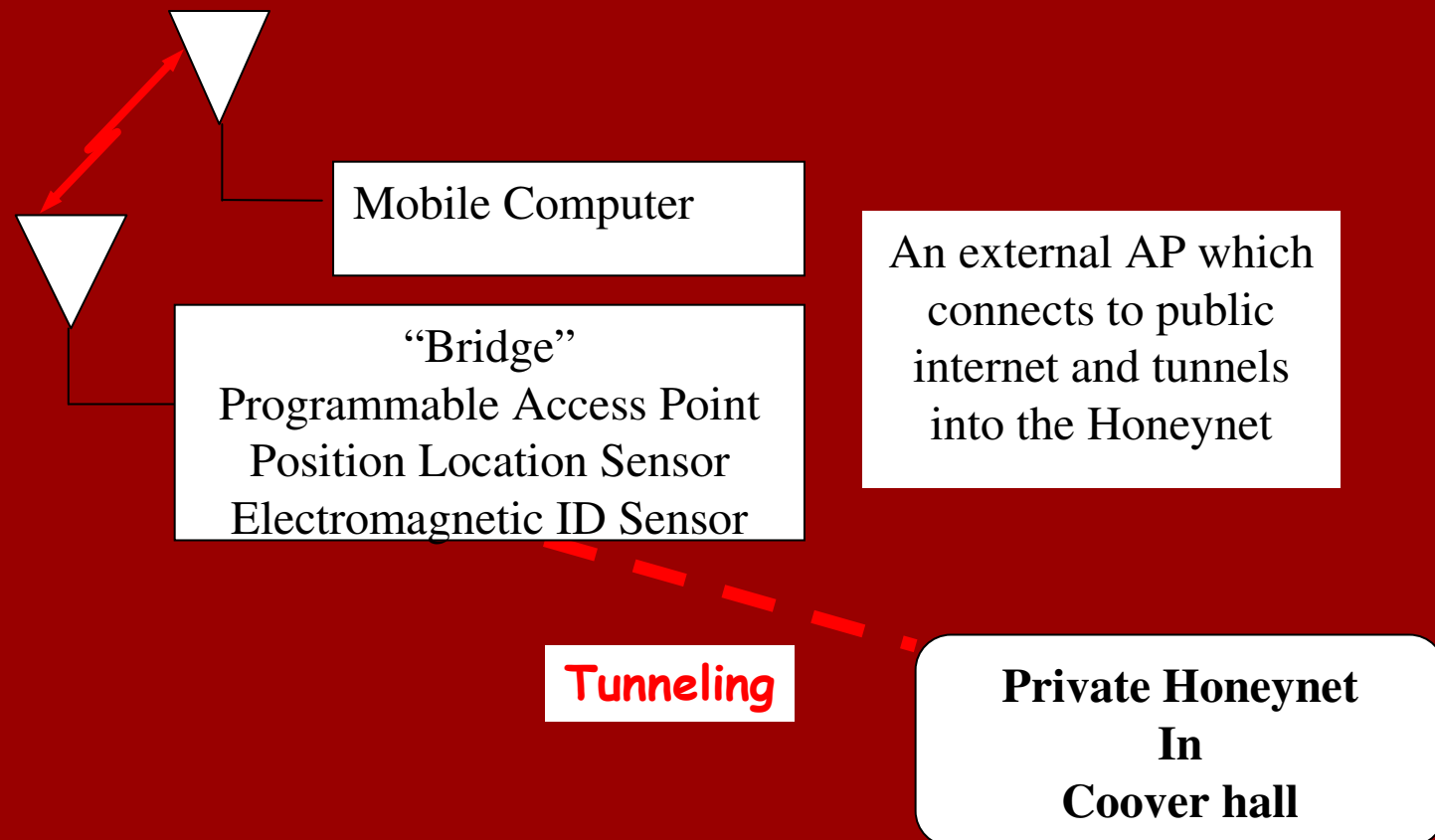


- Information from "bridge" is tunneled back to the Honeynet Private Network

Honeynet Impostor Bridge



Wireless Honeynet – Tunneling Connection



Wireless Honeynet Summary

- Decoy Network
- Control Network
- Data Collection – Attack Analysis
- Honeynet System
- Jamming
- Position-Location
- Electronic Fingerprinting

?QUESTIONS?

Steve F. Russell
Associate Professor
Iowa State University
Ames, Iowa
sfr@iastate.edu
October 27, 2004

ACRONYMS

- AAA - Authentication, Authorization, Accounting
- ACL - Access Control List
- AP - Access port (network)
- EAP - Extensible Authentication Protocol (IEEE 802.11i). Wireless LAN security protocol that uses RADIUS -
- MAC - Medium Access Control
- MIC - Message Integrity Check
- NAS - Network Access Server
- PAP - Password Authentication Protocol
- PSK - Pre-Shared Key (WPA for home or small office - master key)
- RADIUS - Remote Authentication Dial In User Services (IETF standard RFC 2058)

ACRONYMS (cont)

- SSID - Service Set Identifier (for wireless LAN)
- TKIP - Temporal Key Integrity Protocol (Wi-Fi Protected Access)
- VPN - Virtual Private Network
- WLAN - Wireless Local Area Network
- WPA - Wi-Fi Protected Access (a subset of IEEE 802.11i)

Wireless Security Technologies and Policies

- Physically secure access points (reasonably)
- Turn off SSID broadcasting
- Avoid default SSID names
- Enable WEP or WPA or IEEE 802.11i
- Enable dynamic key exchange (if available)
- Enable user authentication
 - **RADIUS authentication**
 - **Username, password, certificates, etc**
- Enable rogue access point detection
 - **Use wireless sniffing**
 - **Port 80 scanning**
- Use only static IP for all devices

Wireless Security Technologies and Policies (cont)

- Use firewalls where ever possible
- Use Virtual private networks
- Use two-way (mutual) authentication
- WEP – Wired Equivalent Privacy
 - **Use automatic WEP key rotation**
- WPA – WiFi Protected Access
 - **Temporal Key Integrity Protocol**
 - **Message integrity check**
 - **Extended initialization vector**
 - **Pre-Shared Key for home and small office**